Course: **Computer Crime-Fall 11**
Instructor: **Professor Ohm**
Date: **12/12/2011**

Exam Notices:

Please read these instructions carefully before proceeding.

1. The examination consists of five (5) pages, including the pages containing these instructions. You will find **two** problems. Please make sure that your copy is complete and that you answer both problems.

2. This is a take-home examination; you have six (6) hours to complete the exam.

3. The exam is worth 250 total points. Problem One is worth 100 points and Problem Two is worth 150 points.

4. Answers will be graded based on content, clarity of expression, and organization. I suggest that you spend time outlining your responses before you start to write. Where information is not provided that would be relevant to the analysis, feel free to explain how different facts would lead to different outcomes.

5. Assume that all cases that were pending when we discussed them in class are still undecided. If any cases have been decided during the course of the semester, you are not responsible for knowing the final rule, result or reasoning, and you will gain nothing by talking about the new decision.

6. You are responsible for the versions of the statutes we studied in this class as they appear in the appendix at the end of the casebook.

7. In answering these problems, you may consult any written materials you wish. You may also consult electronic materials stored locally on your computer and any materials hosted on our class website, http://paulohm.com/classes/cc11/. You may not use the Internet to discuss the exam or assist you with the exam in any other way.

8. Regardless of when you return the exam, you may not communicate with any other student in our class *for any reason* prior to the time when the exam is due. In addition, you may not communicate with anyone else (e.g., students in other classes, family members, other professors, etc.) about the exam prior to the time when the exam is due.

9. Each problem has a separate word limit, indicated at the beginning of the problem and as follows: Problem One: 1500 words and Problem Two: 2500 words. Please put the number of words you write at the end of each answer.

10. If you are hand writing the exam, please write on only one side of each page.

11. Good luck!

Problem One
(100 Points, 1500 Words Maximum)

A very small percentage of people in the world suffer from sound-induced seizures. These people are typically sensitive to repetitive, loud sounds. At least one dozen support websites have sprung up for these people, and most of these websites host message boards on which anyone can post.

One such website is SeizureSupport.com, one of the most popular such websites on the web. SeizureSupport.com hosts a very active message board called *Sound-Sensitive*, dedicated specifically to those who suffer from sound-induced seizures.

Recently, an anonymous user posted a message to the *Sound-Sensitive* message board containing a link. Those who clicked on the link were redirected to a website that seemed to pull up only a blank page but, in reality it installed a piece of software on the user's personal computer by exploiting a previously-unknown vulnerability in popular web browsers.

The secret piece of software was a virus that, once installed on a victim's computer, would periodically play a sound file, one which it appears had been carefully engineered to trigger sound-induced seizures in susceptible people. Whenever it played the sound file, the virus would also turn on the computer's webcam, if present, and broadcast a stream of live video of the person in front of the computer to a separate website hosted at the URL http://cruelty.net. The cruelty.net page was not password protected, meaning it could be viewed by any member of the public. According to records later obtained from the time between when the virus was first distributed until the time the website was shut down, dozens of people logged in to look at the many video streams of victims.

After word of the virus got out and the public learned of the use of SeizureSupport.com as a distribution site, usage of SeizureSupport.com plummeted. Within one month, SeizureSupport.com was forced to shut down its services.

By tracing logfiles found on seized servers, the FBI identified Danny Dingbat, a 22-year-old living in Longmont, Colorado, as the person who had posted the virus-containing message to the *Sound-Sensitive* message board. Dingbat did a lousy job covering his tracks, and FBI experts are convinced he is the one who released the virus. A forensic analysis of Dingbat's computer further revealed that he had on many occasions visited the cruelty.net website where the video streams of victims could be viewed.

Shortly after Dingbat's arrest, the news media discovered a public website run by a loosely-organized, anarchic group calling itself Unattributed. On this website, someone had posted a webpage calling for Unattributed members and admirers to join them in "griefing" people who suffer from sound-induced seizures. The webpage contained a link for downloading a virus, and subsequent FBI analysis proved that this virus was the exact same, forensically identical virus to the one used by Dingbat.

The webpage talked of how it "might be fun" to post the virus to different message boards to attract people susceptible to sound-induced seizures. It also compiled a list of such websites, and included on the list a link to the precise SeizureSupport.com *Sound-Sensitive* message board apparently used by Dingbat.

Once word of this webpage got out, the administrators of some of the websites listed, fearing for their users, began to implore Unattributed to take down the page and asked the FBI to intervene. To date, Unattributed has not responded to these requests and many of these sites have disabled their message boards for fear of spreading the virus further.

The FBI charges Dingbat with committing 1030(a)(2)(C) and 1030(a)(5) of the Computer Fraud and Abuse Act.

In separate litigation before the same judge, the U.S. Attorney files for a protective order against Unattributed, ordering the forced takedown of the webpage. Unattributed, through its lawyer, files a motion arguing that the order should not issue, citing the First Amendment.

You are the law clerk to the judge assigned to both cases. Write a bench memo assessing (a) the strength of the government's case against Dingbat, including a discussion of any possible defenses; (b) an analysis of the type of sentences Dingbat might face if convicted; and (c) whether the judge should issue the injunction.

Problem Two
(150 Points, 2500 Words Maximum)

MyMood.com is a popular new service which allows users to share information about their moods with other people. The key element is a small piece of consumer electronics hardware called the MoodMonitor, a tiny plastic box strapped to a user's wrist or worn behind the ear.

The MoodMonitor contains many miniature sensors that measure biometric values such as pulse, body temperature, sweat production, blood flow, and even (to a limited extent) brain wave activity. MyMood.com's scientists have developed algorithms correlating the data generated by these sensors into surprisingly accurate, minute-by-minute reports of a person's mood. For example, the MoodMonitor can accurately tell whether a user is happy, sad, anxious, fearful, or asleep, and in some cases whether he is lying or telling the truth.

The MoodMonitor also contains a cellular radio chip which can be used to wirelessly upload MoodMonitor data to the Internet. MyMood.com users use this data in at least two ways. First, by default, each MoodMonitor sends a periodic stream of mood data to each user's personal account, information which is stored in a private "mood store" accessible only to the user. By default, this data is sent once every hour, but the frequency can be varied. A user can use the data in his mood store, for example, to generate charts of personal happiness or sleep patterns over time. Old mood information in a mood store is never deleted, meaning the mood

stores for some users contain mood entries for as many as four years, the length of time the service has existed.

Second, when a user presses a small button on his MoodMonitor, a small message is posted to his "MoodTracker," a personalized website accessible only to other people who have the correct password—typically the user's friends and family—but not accessible to the public. A visitor to a MoodTracker sees a series of updates that say, for example, "On Monday, December 5, 2011, John Doe was happy." MyMood.com customers can configure their MoodTrackers to send all updates to friends via email as well. When a user enables this configuration, every time he presses the button, MyMood.com's servers compose a mood update and send it out using standard email protocols to all of that user's friends' email addresses.

Both online services are free, but users pay between $59 and $139 to purchase the MoodMonitor itself, depending on the features desired.

One MoodMonitor user is Deacon Didit. The police suspect that Didit played some role in a recent bank robbery. Despite having undertaken a lengthy investigation, the FBI (who have jurisdiction over the crime, a federal offense) have almost no direct or circumstantial evidence tying him to the crime. They call him in for an interview, hoping to get him to confess or trap him in a lie.

In the interview, Didit claims that at the date and time of the robbery he was skiing on the side of a mountain at a resort five hundred miles from the victimized bank. He remembers the day well because it fell in the middle of a record-breaking cold snap in that area. Despite the best efforts of the police interrogators, Didit says nothing during the interview that implicates him in the crime.

During the interview, one agent notices that Didit is wearing a MoodMonitor behind his left ear. The police wonder whether MyMood.com might store information relevant to their investigation.

You are the Assistant United States Attorney assigned to support the FBI bank robbery unit. The FBI would like to make five types of requests to MyMood.com. They want to obtain records of (1) temperature readings from the date and time of the bank robbery to see if they contradict the skiing alibi; (2) truth records from the date and time of the interview, to see if he was lying; (3) all "mood updates" recorded by MyMood.com's automated logging service; (4) updates posted to Didit's "MoodTracker" website; and (5) records of the average mood updates recorded for men of Didit's age across all of MyMood.com's customers, to serve as a baseline for comparison. The FBI would also like (6) to order MyMood.com to increase the frequency with which Didit's MoodMonitor sends data to his mood store from once every hour to once every minute.

Write a memo to your boss, the United States Attorney, advising her on how the office should approach these requests. Discuss whether any of the information sought falls under Fourth Amendment or statutory privacy protections. For covered information, talk about the form requests should take to satisfy constitutional and statutory concerns. Point to specific statutory provisions, case law, or policy

arguments relevant to your analysis.